(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
11 October 2001 (11.10.2001)

PCT

(10) International Publication Number
WO 01/75705 A1

(51) International Patent Classification[7]: G06F 17/60, G08B 13/14

(21) International Application Number: PCT/GB01/00959

(22) International Filing Date: 6 March 2001 (06.03.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
00302714.1 31 March 2000 (31.03.2000) EP

(71) Applicant *(for all designated States except US)*: **BRITISH TELECOMMUNICATIONS public limited company** [GB/GB]; 81 Newgate Street, London EC1A 7AJ (GB).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **HOPKINS, Jonathan** [GB/GB]; 3 The Glebes, Snape, Saxmundham, Suffolk IP17 1QF (GB). **MCGLAUGHLIN, David, Caldwell** [GB/GB]; 19 Grange Road, Ipswich, Suffolk IP4 1NP (GB). **BRENNAN, Alexander, Charles, Croxall** [GB/GB]; 55 Cobbold Street, Ipswich, Suffolk IP4 2DN (GB). **BLYTH, Richard, Charles** [GB/GB]; 53 Marlborough Road, Ipswich, Suffolk IP4 5BA (GB). **REEDER, Stephen, Michael** [GB/GB]; 6 Luxborough Grove, Furzton Lake, Milton Keynes, Buckinghamshire MK4 1LX (GB).

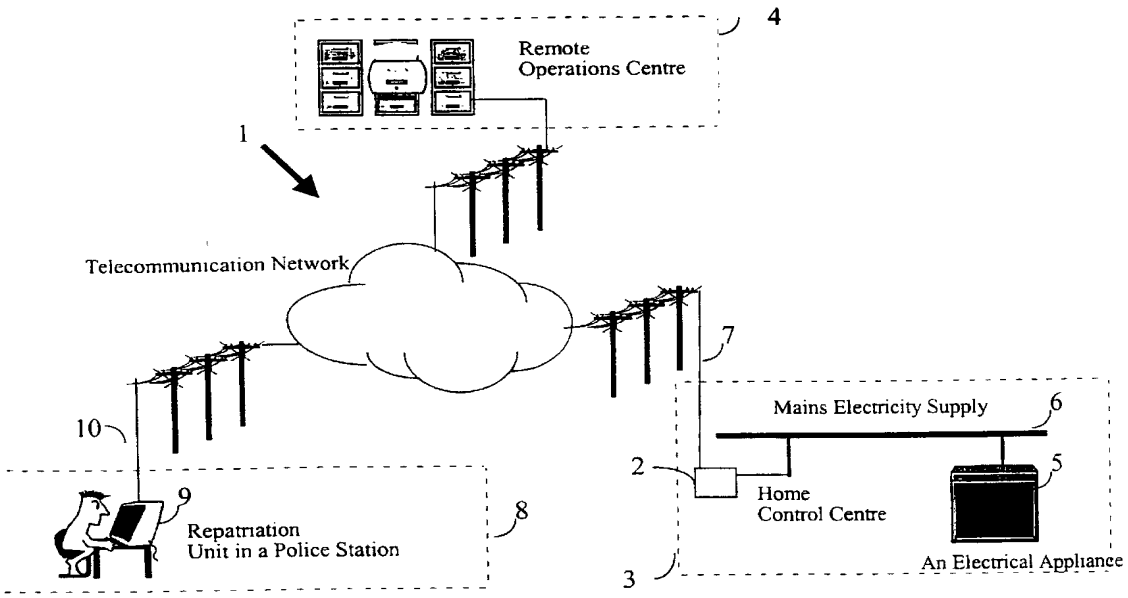
(74) Agent: **BRADLEY, David, William**; BT Group Legal Services, Intellectual Property Department, 8th Floor, Holborn Centre, 120 Holborn, London EC1N 2TE (GB).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE,

[Continued on next page]

(54) Title: ELECTRONIC COMMERCE



(57) Abstract: In an electronic commerce system a point of sale device on receiving a customer transaction order initiates the programming of the device with a permission code. The permission code is specific to a customer location. At least some of the capabilities of the apparatus are then inhibited until and unless a corresponding permission code is supplied to the customer apparatus when installed at the customer location.

WO 01/75705 A1

IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

Published:

— *with international search report*

Electronic Commerce

The present invention relates to a system that enhances the security of apparatus traded using electronic commerce.

The term "electronic commerce" is used in this document broadly to encompass trading systems using information and communication technologies. It includes, both on-line retailing via the public Internet, and electronic point of sale (EPOS) systems used on conventional retail premises. Furthermore, it encompasses systems where the underlying network technology may be, for example, optical rather than electronic.

Increasing numbers of goods are being sold using electronic commerce systems. In the case of on-line trading via the Internet, the delivery of goods may often involve long and complex supply chains. It is not unusual for goods manufactured in one country, for example, Japan, to be ordered from a retail website in another country, for example the US for delivery to a third country, for example the UK. In such cases, theft of goods in the supply chain is potentially a serious problem. This problem is compounded by the possibility of some part of the electronic commerce system being "hacked" giving thieves knowledge of the impending delivery of high value goods to a certain destination. Even where less extensive electronic commerce systems are involved, such as a local area network in a retail outlet using EPOS terminals, there is still a risk of goods being stolen prior to being installed at the customer premises.

According to a first aspect of the present invention there is provided a method of operating an electronic commerce system, including:

a) receiving at a point of sale device a customer transaction order for a customer apparatus, and

b) subsequently conveying the customer apparatus to the customer,

characterised by a step initiated at the point of sale device of programming the customer apparatus with a permission code specific to a customer location and in that at least some of the capabilities of the apparatus are inhibited until and unless a corresponding permission code is supplied to the customer apparatus when installed at the customer location.

The term "point of sale device" encompasses, for example, an e-commerce web server carrying out transactions remotely over the Internet with the customer as well as an EPOS terminal used with the customer physically present as in the specific embodiment described below.

The invention significantly enhances the security of the supply chain, by programming goods at the point of sale with a security code. Once programmed, the goods can only become fully operational if the corresponding code is supplied to the apparatus. Accordingly, the value of the apparatus to any third party who does not have the corresponding permission code is greatly reduced.

Preferably the data identifying the customer is read from a transaction card holding customer account data.

Another important advantage of the present invention in its preferred implementations is that it is able to enhance the security of transaction cards such as magnetic stripe cards or smart cards arranged to function as debit cards or credit cards. Using this aspect of the invention, even if such cards are stolen, they are of little value to the thief, since goods purchased with the card will only function at the location associated with the true owner o the card. The data used to identify the customer in these cases, may be the credit card account data itself, typically comprising an account name and a card number and expiry date. Alternatively, the card may include additional information specifically for use in programming the apparatus. The data may be validated against biometric data such as an iris print, a voice print or a thumb print.

Preferably the method includes reading at the point of sale device data identifying the customer, and communicating to a remote operations centre connected to the electronic commerce system by a communications network a request for the said permission code specific to the customer location and receiving the said code from the remote operations centre via the communications network. Preferably, at the customer location the corresponding permission code is received from the remote operations centre by an interface unit in communication with a plurality of customer apparatuses.

In published European Patent Applications Nos. 675626 and 960407 the assignee of the present invention has disclosed improved security systems using an interface ("Home Control Centre") between the public switched telephone network

(PSTN) and appliances in customer premises whereby such apparatus may be less attractive to thieves since without certain permissions obtained by way of the PSTN from a remote operations centre the appliance will not function.

In further developments of the system of EP960407 disclosed in co-pending European patent applications Nos. 99302132, 99302133, 99302134 and 99302149 alternative communications methods for both communication within the customer premises and communication between the home control centre and a permission granting arrangement were disclosed.

In yet a further development disclosed in co-pending European Patent Application no. 99307981, the customer premises interface was developed to provide an environmental alarm arrangement for simple installation and use in communal premises, for example to provide smoke or fire detection in an apartment block.

A brief introduction to the earlier arrangement and its operation will facilitate understanding of the invention hereinafter disclosed and claimed. However, for a full description of the operation of the basic system the reader should refer to the earlier applications referred to above.

Thus referring to Figure 1, in one form a control and communications network uses the PSTN 1 to effect communications between a remote operations centre 4 and customer premises 3. It will be appreciated that for simplicity only one remote operations centre is shown although there may be many such centres distributed across the PSTN.

In each customer premises 3, a home control centre 2 provides an interface for communication on the one hand by way of the customer telephone line 7 and the PSTN with the remote operations centre and on the other hand by way of the mains electricity supply 6 of the customers premises 3 with suitably adapted electrical appliances 5.

Although reference in the earlier application was to the two forms of communication mentioned, that is by superimposition of signalling on the supply line 6 and by way of the PSTN, it is noted that other communications arrangements have been proposed by the proprietor of this application including but not limited to use of cellular radio networks, satellite communications and radio and Internet links between the home control centre 2 and the remote operations centre 4. Communication

between the home control centre 2 and appliances 5 may be by way of low power radio such as DECT, by way of an Intranet or by way of telephony wiring for example.

Also shown in Figure 1 is a repatriation unit 8 which enables stolen property to be identified by authorised persons for return to the owner. It will be appreciated that other control centres accessible by way of the PSTN may also benefit from the arrangement.

According to another aspect of the present invention, there is provided point of sale system for use in electronic commerce characterised by a programming data interface for connection to a customer apparatus and arranged to programme the customer apparatus with a permission code specific to a customer location whereby, in use, least some of the capabilities of the customer apparatus are inhibited until and unless a corresponding permission code is supplied to the customer apparatus when installed at the customer location.

The point of sale system may comprise a point of sale device (as broadly defined above) together, optionally, with ancillary systems connected to the point of sale device. For example the point of sale system might comprise an EPOS terminal and a programming unit located in a stock room away from the EPOS terminal and arranged to programme the apparatus, for example via a power supply signalling interface.

An electronic commerce system in accordance with the invention will now be described by way of example only with reference to the accompanying drawings of which:

Figure 1 is a block schematic diagram of a communications and control network;

Figure 2 is a block schematic diagram of the home control centre of figure 1 modified to provide additional features of the invention;

Figure 3 is a block schematic diagram of adapted consumer premises apparatus;

Figure 4 is a flow chart showing the operation of the home control centre of figure 2;

Figure 5 is a flow chart showing the operation of relevant circuits of the consumer premises equipment of figure 3;

Figure 6 is a block schematic diagram of apparatus in the remote operations centre;

Figure 7 is a flow chart showing functionality of the operation of the remote operations centre of Figure 1;

Figure 8 shows a flow chart of an information request response in the remote operations centre;

Figure 9 shows operation of a capability change section of the operations centre;

Figure 10 shows a further flow chart in relation to a keyed changed request from a home control centre to the remote operations centre;

Figure 11 shows a flow chart of a part of an EPOS terminal;

Figure 12 shows operation of the processor of the apparatus of Figure 3 in respect of a specific function request: and

Figure 13 shows a block schematic diagram of an EPOS terminal modified in accordance with the invention.

Figure 1, to which reference has already been made, shows an implementation of a communications and control network of the kind modified by the present invention and as disclosed in European patent application number 960406. A detailed explanation of the arrangement shown in Figure 1 may be had by reference to the previous application in respect of coding of electrical appliances 5 and only a limited description of the functionality of the remote operations centre (ROC) and home control centre (HCC) in respect of the prior art will be given herein.

Referring to Figure 2, the HCC 2 of Figure 1 comprises a processor 23, with associated data stores 24, 26. As described hereinafter, the processor has an analogue shift key (ASK) signalling interface 25 for communicating on the mains electricity supply 6. For completeness it is noted that the ASK interface 25 may be replaced by other signalling arrangements communicating by way of the mains electricity supply. In alternative arrangements radio transmission or Intranet or telephony line communication may be used in place of the ASK interface 25 or in addition thereto. Thus, whilst herein communication is described as being on the mains electricity supply to electrical appliances and/or detectors and/or sensors, it should not be taken as limiting the invention to communication by way of the electricity supply.

The processor is also shown as having access to a tone generator modem 22 for communication by way of network termination equipment 20 to telephone lines 7. again, while herein communication is described as being by way of the telephony network and location data is derived from calling line identity (CLI), it should be appreciated that other communications methods and location identification may be used including, but not limited to, used of cellular networks for communication including triangulation between cellular network masts to determine the location identity. Low Earth orbital satellite and/or direct radio communication between the HCC 2 and ROC 4 may also be used while global positioning by satellite (GPS) and/or burnt in identification of the HCC 2 should not be considered to be excluded.

Furthermore, in descriptions hereinafter relating to modified appliances and/or sensors and/or environmental alarms and the like, while a specific form of communication between such devices and the HCC may be specified these should not be taken as excluding other forms of communication.

Referring now to figure 3, in a protected or controlled appliance (e.g. 5 of Figure 1), modification of the process control 15 within the appliance (which may be any electrically operable or electro mechanically assisted device) requires the process control to signal to operational circuits of the appliance.

Thus the process control 15 has an ASK interface 14 for communicating by way of the electrical main circuit 6 with the HCC 2. The HCC 2 returns control information to the process control 15 by way of the mains electrical circuit 6 and the ASK interface 14 to permit or deny activation of operational circuits. As discussed in the earlier European patent applications mentioned above, one method of discouraging theft is to have the power supply of the appliance 5 cease to supply power to the operational circuits unless or until the process control 15 has received an appropriate code downloaded from a ROC by way of the HCC 2. Thus initially, the device until coded forwards a message to the electrical power supply circuit 6 each time it is connected requesting a coding. Once connected in premises at which a HCC exists then it will receive coding with which it will compare subsequently received codes prior to operation. On first coding it will also receive a "blanking" code which is know only to the coded appliance and to the ROC, the blanking code being transmitted to the HCC only on specific request of a legitimate authority

(owner) to enable decoding of the appliance to permit its bona fide transfer to another party.

In the present invention, in addition to receiving operation and blanking codes, the HCC also includes the ability to transfer additional information to the process control 15 this information including identity of "capability sets" and timer information. The capability sets are programmed in to a memory 19 and define which functions of the appliance are available for use. For example, in a television set, the channels available to be used may be held in the capability set along with times at which such channels are to be available. Thus when a function is requested by use of a keypad or remote control handset, indicated by function select 13, the process control may determine from the capability set in combination with other factors such as time of day or day of week whether the appropriate function is available. The process control may thus permit or refuse activation of the appropriate function which enables the functionality of the apparatus to be varied from the ROC 4 by way of the home control 2 to the process control 15.

This facility therefore allows service providers, for example satellite or terrestrial broadcast television service providers, to permit or deny access to certain channels by way of a secure route. Further, the arrangement permits parental control of times and channels available for example.

A further advantage of the arrangement hereinafter described is that appliances may be coded through the supply chain from manufacturer, to wholesaler, to retailer, to end customer so that theft in transit is more difficult and electronic sales (for example by way of the Internet) can be secured. Thus even if an attempt is made to purchase goods or services using fraudulent means, for example by quoting another person's card account number or by using a stolen credit or debit card, the goods will be of no benefit to the fraudulent user since they will be pre-coded at the point of sale to the specific premises of the proper card owner. In this way, delivery of electrical goods to a specific address is secured since any theft will leave the thief with an unusable apparatus which is readily traceable to its proper owner and which may reveal its location to proper authorities to facilitate recovery.

Turning now to figure 4, the processor 23 of the HCC 2 of Figure 2 is normally quiescent in a main state 900 until it receives, by way of the mains electrical circuit 6, an "unlock request" message (901) from an appliance 5. The

message includes the identity of the requesting apparatus by type, manufacturer and electronic serial number. If the requesting apparatus is not in the list of appliances held in the volatile data store 24 then by way of the path 906 to 970 coding is requested from the ROC 4 by way of the PSTN 1. Various checks are made to ensure that the requesting appliance codes appropriately and that the new equipment is now included in the appliance list. Full details of this part of the operation are disclosed in the earlier published European applications, including a more complete flow chart for those operations involved after the commencement of the Lock Enable Timer at step 910.

Assuming that the requesting apparatus is in the list held in the data store 24 then at step 903 the message type is analysed to determine how the message is to be handled by the HCC. If the message is an environmental alarm (944) then it is handled in a manner described in other co-pending patent applications of the proprietor to ensure that appropriate response to the alarm occurs. This is indicated here for the sake of completeness only.

Similarly, if the message indicates a basic type appliance (that is one coded only for the purposes of permission to operate when re-connected to power after disconnection) then the Signal Group Basic route 945 is followed. Thus at 946 a check is carried out to determine whether in respect of the particular appliance the blanking code is present and, if so, the equipment is ordered to decode itself as disclosed in published European patent application no 960407 which includes a full flow chart in respect of the code blanking activity.

However, if at step 946 the blanking code is not present, this being the more usual status, then the unlock code is recovered from the data store (904) and is transmitted as an unlock response (905) to the mains electrical supply 6. It should be noted that where a precoded appliance (from an electronic sale record) is first connected to a supply in the premises 3 its unlock code will already be present in the equipment list of the HCC 2 provided that the equipment is licitly present in the premises and that the HCC has either made a connection to the ROC 4 in the period between coding and delivery and connection or has been forced to make such a call by the owner causing a reset of the HCC 2. In the alternative, where the equipment is licitly present in the premises, when the HCC receives an unlock request it will follow the path indicated at step 902 and the ROC 4 will recognise the coding

request and return the appropriate (already stored) coding for the appliance to operate.

It will be realised that if the ROC receives a coding request from apparatus in an incorrect location it may not return a valid coding and may cause an alert to be provided to appropriate authorities. However, there may be advantages in allowing the apparatus to operate on a temporary basis, for example by returning a coding with a short time decay (hereinafter discussed) so that a fraudulent operator of the appliance may not realise that the authorities are aware of the illicit operation and its location.

Returning once again to step 903, if a signalling group information message is received indicating a request for capability set information more detailed than a simple authorisation code, then at step 947, the processor 23 determines whether there are instructions for the apparatus in the list. If at step 947 instructions exist then the information message is returned through the ASK interface 25 at step 952 and the HCC resumes its quiescent state.

Now, if at step 947 instructions in respect of the particular apparatus have not previously been received and stored then a call is established through the PSTN to the ROC 4 and an equipment information required message is transmitted (948). The ROC 4 will respond with an equipment information response message (949) and the processor 25 determines whether the message includes information to be stored either in respect of the particular request or additional thereto (950). If not then the received information is passed through the ASK interface to the mains as a transmit information message (952) prior to the quiescent state being resumed.

If the received message from the ROC 4 includes information to be stored then the list held in the data store 24 or 25 is updated (951) in accordance with the message and the information responding to the request received is then transmitted as before at step 952.

Considering now the operation of process control 15 of figure 3 and referring also to figure 5, from a quiescent state 50, the process control may be interrupted or triggered as a result of user action or as a result of timer permissions decaying to zero. Considering first the re-connection (or first connection) of electrical power to the apparatus, as indicated at step 51, the process control causes an Unlock Request Message to be transmitted 52 and commences a cover timer 53 for response from

the HCC 2 as previously described with reference to Figure 4. Four potential exits from the timer waiting state may be received representing respectively the outputs of the HCC 2 of System Lock Enable (909), Blank Instruction (912), Unlock Response (905) or the internal timer of the appliance expiring with no response being received. The process followed in respect of each of these responses to an Unlock Request (SG Basic) message is fully disclosed in the prior published European Patent Applications mentioned hereinbefore and further description here is not deemed necessary.

Turning to the other possible exits from the quiescent state 50, the user may force a request to the HCC 2 by activating a reset function either directly or through remote control in order to activate or de-activate a capability in the controlled apparatus. Thus if the user has made arrangements with a supplier to allow additional functionality or reception of an additional television channel from a service provider, resetting the system (56) causes an SG Plus message (57) to be transmitted by way of the ASK interface 14 to the mains supply line 6 and thence to the HCC 2. Following transmission of the request message a cover timer is started (58) while awaiting the response from the HCC 2. If, as expected, an information message is received (59) (transmitted as hereinbefore described at 952 of Figure 4) then any additional capability set "Y" may be stored as active in the data store 16 together with an appropriate timer associated therewith (if any) at step 61.

Alternatively, if the information message received includes a multiple capability set activate and/or deactivate instruction (possibly with respective associated decay timers) then these are stored at as indicated at steps 62 and 63.

A further facility which may be provided by the control system of the invention allows for sensors to be provided which may be smart card, smart badge, or passive or biometric sensors so that the presence or absence of a particular card or badge may be used to modify or determine the facilities provided. Thus, as indicated at step 64, if there is a change in the card presence this may cause the process control 15 to generate an SG plus message as before following the steps 57 et sequenda.. This enables the particular apparatus to provide certain facilities only when an appropriate card is present. Thus a television set or video may have certain capabilities turned off unless a card indicative of adult presence is present such that parental control of channels viewed for example may be effected.

Sensor presence may also be a limited period authorisation such that the timer decays and causes a further SG Plus message to be transmitted as indicated at step 65. On one of the timers decaying to zero in the data store 16 and process control 15, the associated capability set "X" is marked as disabled (66) and a message transmitted as before. This will result either in an information message including a renewed time for the capability set or a disable message as appropriate through steps 59 to 63.

Note that if the cover timer started at step 58 expires (67) without an information message being received then the process control assumes that the previous capability set authorisation pattern remains in force minus any capability set (step 68) which for which the respective timer decayed to zero.

In the absence of an information message the process control may set a further timer to force an SG plus message at a subsequent time to attempt an update of the capability sets.

Turning now to figure 12 while continuing to refer to figure 3, if, through the function select entry 13, a function is requested then the process control reads the current capability set(s) which are active (step 71) and determines whether the particular function is controlled (step 72). If the function is an open function ("Always") then as indicated at step 73 the function is implemented and the controlled appliance responds to the function request appropriately. If the function is disabled ("Never") then a record of the request may be entered in an exception log (step 74) and a display activated (step 75) indicating that the function is unavailable.

The third possibility is that the capability set requires that the function requested is "authorised" each time it is activated. Thus at step 76 an information request message is transmitted to the HCC 2 and a cover timer started (77). On receipt of an information response (78) the process control will store any modification to the capability set authorisation (with a decay timer if present) and will again read the capability set. If the timer set at step 77 expires then the process control may check the number of attempts made (step not shown) and will either return to reading the capability set or will step to reject the request.

Note that for any particular function request the number of attempts to check authorisation may be bounded so that only a single request for information is made in respect of the function requested and if not authorised the requested

function may be rejected. It will be appreciated that the cover timer started at step 77 must be sufficient in some circumstances to allow for the HCC to effect a modem interchange with the ROC in case there should be a third party authorisation entered through the remote centre.

Referring now to figure 6, the ROC in its simplest form comprises a computer 30 with associated data storage 31 and communications capabilities represented by telephone lines 37 and modems 33. Location detection represented by CLI detector 32 is also provided, noting that GPS may also be detectable. Much of the functionality of the ROC of figure 6 has been described in the proprietors earlier applications such that only a representative selection of program instances are from the previous operational description are shown in figure 7 to which reference is now also made.

Thus the first process shown (811) is a response to a HCC 2 requesting an equipment list. The HCC 2 will lose data from the volatile data store 24 (of figure 2) if power is removed for any reason. It is therefore necessary for the ROC to return a complete listing to the HCC to enable apparatus in the controlled premises to function. Thus at step 812 the location identity is recovered (from CLI detector 32/GPS or wired coding from the message) and a comparison made to determine whether the location is valid (line ID Registered 813). An attempt from an unauthorised source (including an invalid combination of identity and wired coding) will result in the termination of the interchange (816) and a record being made of the call (step 817). Appropriate authorities may be notified of the attempt if there has been an indication that the HCC making application has been fraudulently removed from its previous location.

If there is a valid registration of the requesting HCC then the equipment listing and codings appropriate to the premises in which the home control is located will be loaded (step 814) and encompassed in a message for return through the PSTN (815).

In the Equipment code required (step 820) process, when a request is received 820 then as previously location data is checked (822,823) before location code and equipment code and blanking codes are determined (824, 825). It should be noted here that where a pre-coded appliance (hereinafter described) causes

application for an equipment code and there is an indication of invalid location of the appliance an appropriate action may be taken (steps not shown).

Once codings for the requesting appliance have been determined then an equipment code response is transmitted 827 and a timer for confirmation of coding 826 is started. If on expiry of the timer no response has been received then a further attempt to transmit codings may be made and/or a query may be entered against the record of the appliance in the appropriate equipment list. Assuming that an equipment stored confirm message is received (828) then the cover timer is stopped (829) and the process ended.

Turning now to figure 8, where a message from a HCC 2 to the ROC 4 is an information request (70) as before, the location of the calling control centre is checked (71,72) and if not valid the request rejected (73) and a record of the attempt made (74).

Assuming validity of the information request message then data for the particular location (capability sets, timers, new apparatus) is recovered (75) from the data store 31 and an information response message encapsulating that data is transmitted (76) back through the PSTN.

In figure 9 there is shown a process whereby a service provider or appliance retailer may register changes against a particular customer location. Thus, the supplier forwards a capability change message which is received at the ROC (step 80) and the identity of the supplier checked (81) and validated (82). Assuming that the supplier is appropriately identified the HCC is identified from the message content and a check carried out to ensure that the HCC is registered (84).

If the capability change requested is subject to agreement from the HCC user then a check is made to ensure that the end user has given permission (85) prior to responding to the change request. If the change is simply one requiring a capability set modification then the appropriate information is amended (86) in the data store 31 so that on the next application of the respective HCC for information the amended capabilities are transmitted. A notification message is returned to the supplier at step 87 and the process terminates.

If at step 86 it is necessary to allocate a new item or appliance to the HCC then appropriate codings are generated and stored and these will be notified to the supplier so that the appliance being supplied or sold may be appropriately coded.

If there is any failure of any of the validity or permit checks (82, 84, 85) a non implementation message is transmitted back to the requesting supplier (88) which may include a reason for non implementation and the interchange of information terminates (89). A record of the transaction attempt may be made in an exception log (90).

Figure 13 shows a modified EPOS terminal suitable for implementing the invention. Thus the terminal includes a processor 123 having an associated data store 126. Normal functionality of the terminal is provided by a keypad 128 and swipe card reader 129 combination enabling credit cards to be swiped and credit authorisation to be sought by way of the PSTN through a modem122 and network termination 120 to a telephone line 127. Note that this authorisation step may be omitted if there are arrangements between the card issuer and the operator of the remote operations centre of the invention to effect validation through a more direct communication. A smart card sensor 130 (which may also be responsive to other kinds of identification methods) is provided to enable customer identifying data to be read which data may also identify the customers HCC.

An appliance being sold to the customer is now connected to an appliance coding point 131 which may simply be an electrical socket supplied with normal mains electrical power. This enables the processor to communicate with the appliance through an ASK interface 125.

Now an appliance connected to the mains electrical power, if including the appropriate programming causes a request for code to be transmitted to the mains power line as previously described. This data is captured through the ASK interface 125 by the processor 123 so that any existing coding protecting the appliance through the supply chain can be forwarded to the ROC 4.

Thus as previously discussed with reference to figure 11, once the processor 123 has acquired all necessary data (including the appliance code, customer identity, home control centre identity) it will initiate a call through the tone generator and modem 122 to the remote operations centre 4 and will await a response. Assuming now that the response is an acceptance then the current coding and blanking code for the connected appliance will be received together with the new authorisation code and blanking code for the appliance which codes are now stored at the ROC in the appropriate home control centre list associated with the customer.

The processor 123 uses the received message data firstly to blank the existing coding from the appliance (which may have been present from manufacture) and then to re-code the appliance to the coding provided by the ROC. This coding is again carried out by way of the ASK interface 125 and appliance coding point 131. Once coded, the appliance may be disconnected from the connection socket. Any subsequent re-connection of the appliance other than at the location identified from the credit/smart card and/or biometric identity will result in restricted capability or non-operation of the appliance as hereinbefore referenced.

Turning now to Figure 11, the supplier chain EPOS terminal interchange with the ROC 4 is considered in more detail. Thus, when a sale is being made (91) the customer smart card (specific to premises or credit or debit cards etc.) is used to determine the identity of the customer 92. A check on the validity of the tendered identity and/or PIN entered may be made (93) and any relevant credit authorisation acquired (step not shown). Any failure may be recorded in an exception log (94) and a notification message may be sent (95) to an appropriate third party (Credit issuer, law enforcement agency) .

Assuming now that the transaction is determined as valid (93) then a call is established to the ROC and a capability change message transmitted (96). A response timer is started (97) and a response message from the ROC awaited. If the response message is an acceptance and includes coding information then this is transferred (99) to the appliance by way of its normal communications path, probably through a mains power connection.

Note that if the timer expires a number of attempts may be made to repeat the transaction validation and coding process with the ROC and only if the maximum number of attempts is exceeded (101) is a record made in an exception log (102).

Now if for any reason the ROC returns a not implemented message then a record may be made in the exception log and, depending upon the reason for rejection, appropriate notifications to third parties may be made.

It is here noted that where a service supplier provides capability change information to the ROC 4 the program of figure 11 may simply terminate once an acceptance message is returned since no coding message need be returned.

In a further process available at the ROC 4, referring now to figure 10, where a keyed entry to the HCC 2 is made once the complete change has been identified in

the HCC 2 (process not shown) the HCC transmits a keyed change request to the ROC. Such a request maybe in respect of modification of capability sets, time of availability, availability only on sensed presence and the like whereby user authorities are modified by the user.

Thus when the ROC receives a keyed change request (110) the HCC is identified (111) and the usual identity and validity checks are carried out (112, 113 114). Assuming that the request is valid then the data for the appropriate HCC is recovered (115) from the data bank 31 to enable a check to be carried out (116) on any required PIN entry or smart card presence prior to modification of the respective data and an information message including the updated information being transmitted (118).

For the avoidance of doubt it is here noted that the term HCC should not be construed as limiting the application of the invention to domestic premises since the control mechanisms and methods disclosed hereinbefore may be equally applied to non domestic premises with little variation in the implementation.

CLAIMS

1. A method of operating an electronic commerce system, including

a) receiving at a point of sale device a customer transaction order for a customer apparatus and

b) subsequently conveying the customer apparatus to the customer

characterised by a step initiated at the point of sale device of programming the customer apparatus with a permission code specific to a customer location and in that at least some of the capabilities of the apparatus are inhibited until and unless a corresponding permission code is supplied to the customer apparatus when installed at the customer location.

2. A method according to claim 1 including

reading at the point of sale device data identifying the customer,

communicating to a remote operations centre connected to the electronic commerce system by a communications network a request for the said permission code specific to the customer location and

receiving the said code from the remote operations centre via the communications network.

3. A method according to claim 1 or 2, in which, at the customer location, the corresponding permission code is received from the remote operations centre by an interface unit in communication with a plurality of customer apparatuses.

4. A method according to claim 3, in which the apparatus is connected to a fixed power supply circuit and data is communicated between the interface unit and the apparatus via the said fixed power supply circuit.

5. A point of sale system for use in electronic commerce characterised by a programming data interface for connection to a customer apparatus and arranged to programme the customer apparatus with a permission code specific to a customer location whereby, in use, least some of the capabilities of the customer apparatus are

inhibited until and unless a corresponding permission code is supplied to the customer apparatus when installed at the customer location.

6. A system according to claim 5, further comprising a customer data interface arranged to receive data identifying the customer.

7. A system according to claim 5 or 6, further comprising a remote communications interface arranged to transmit via a communications network to a remote operations centre a request for the said permission code.

8. A method according to claim 2, in which the data identifying the customer is read from a transaction card holding customer account data.

9. A transaction card programmed with data for use in a method according to claim 8.

Fig 1

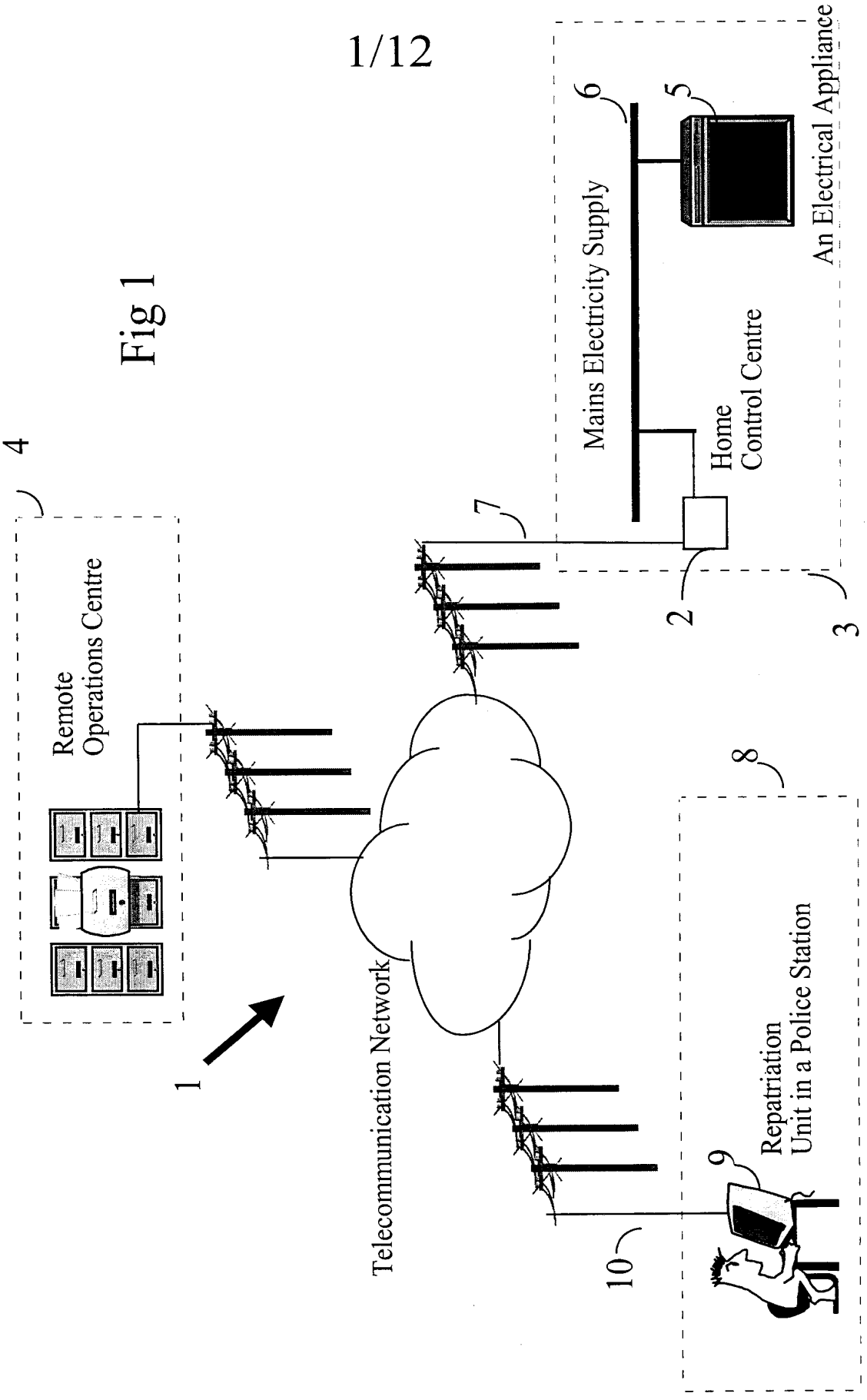

4
Remote
Operations Centre
1
Telecommunication Network
7
Mains Electricity Supply
6
5
An Electrical Appliance
Home
Control Centre
2
3
8
Repatriation
Unit in a Police Station
9
10

Fig 2

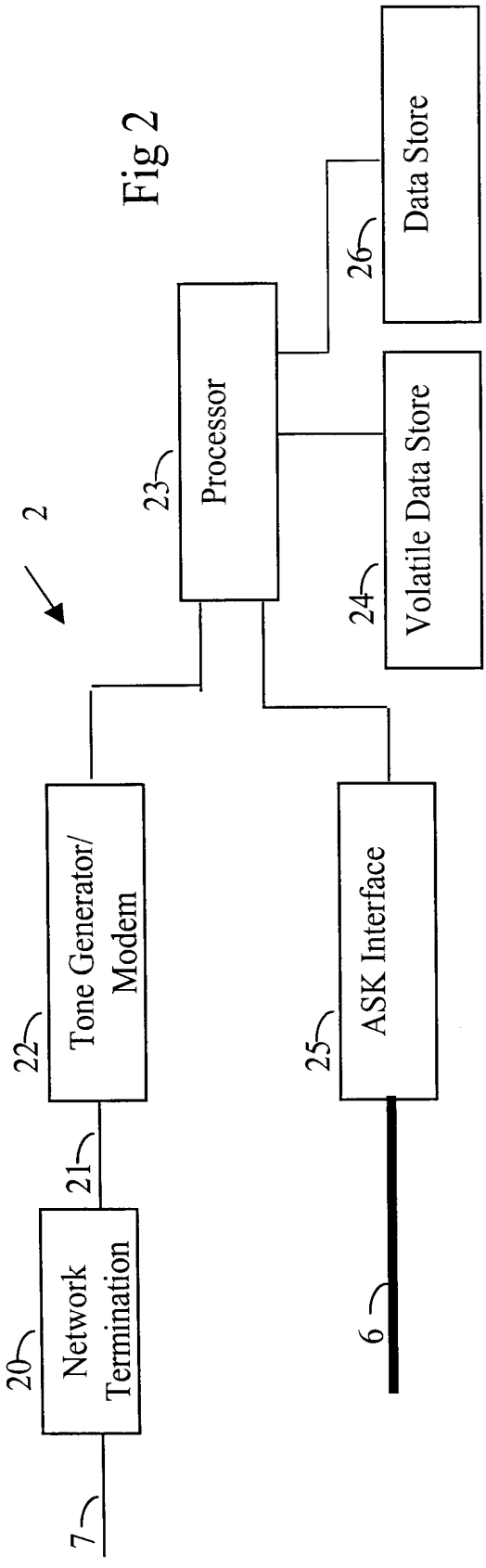
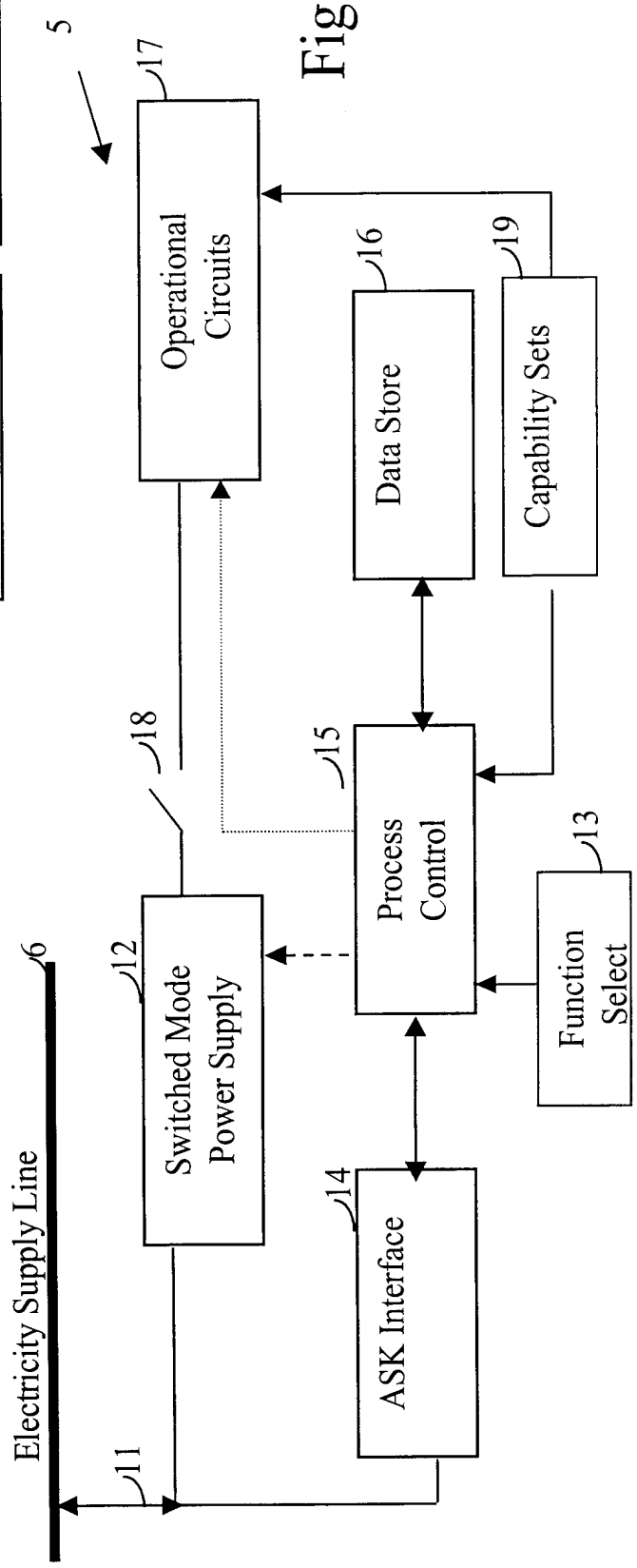

2
23
Processor
26
Data Store
24
Volatile Data Store
22
Tone Generator/ Modem
25
ASK Interface
21
20
Network Termination
6
7

Fig 3


5
17
Operational Circuits
16
Data Store
19
Capability Sets
18
15
Process Control
13
Function Select
12
Switched Mode Power Supply
6
Electricity Supply Line
14
ASK Interface
11

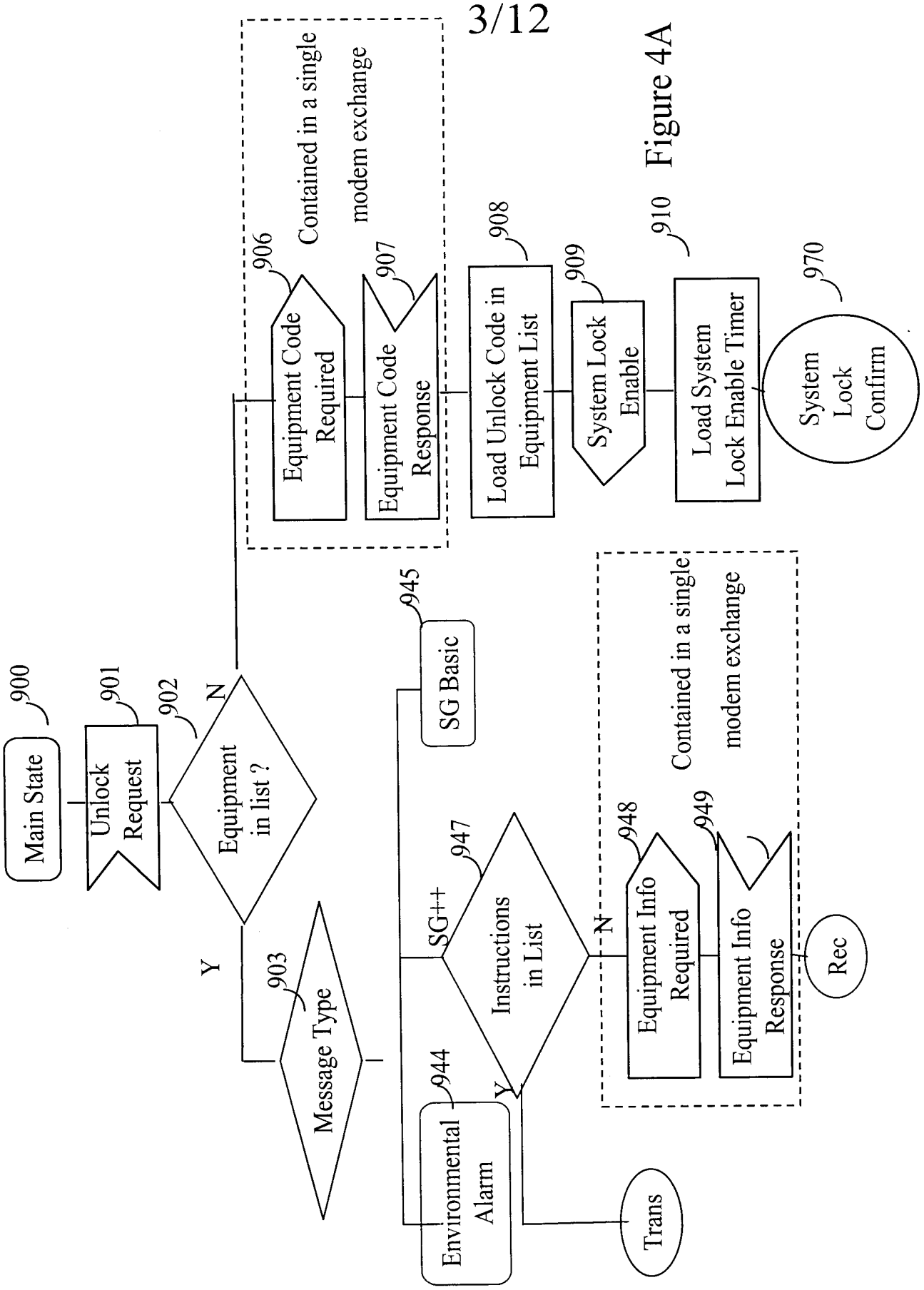

Main State
900
Unlock Request
901
Equipment in list ?
902
N
Y
Message Type
903
Contained in a single modem exchange
Equipment Code Required
906
Equipment Code Response
907
Load Unlock Code in Equipment List
908
System Lock Enable
909
Load System Lock Enable Timer
910
System Lock Confirm
970
SG Basic
945
SG++
Instructions in List
947
Y
N
Environmental Alarm
944
Trans
Contained in a single modem exchange
Equipment Info Required
948
Equipment Info Response
949
Rec

Figure 4A

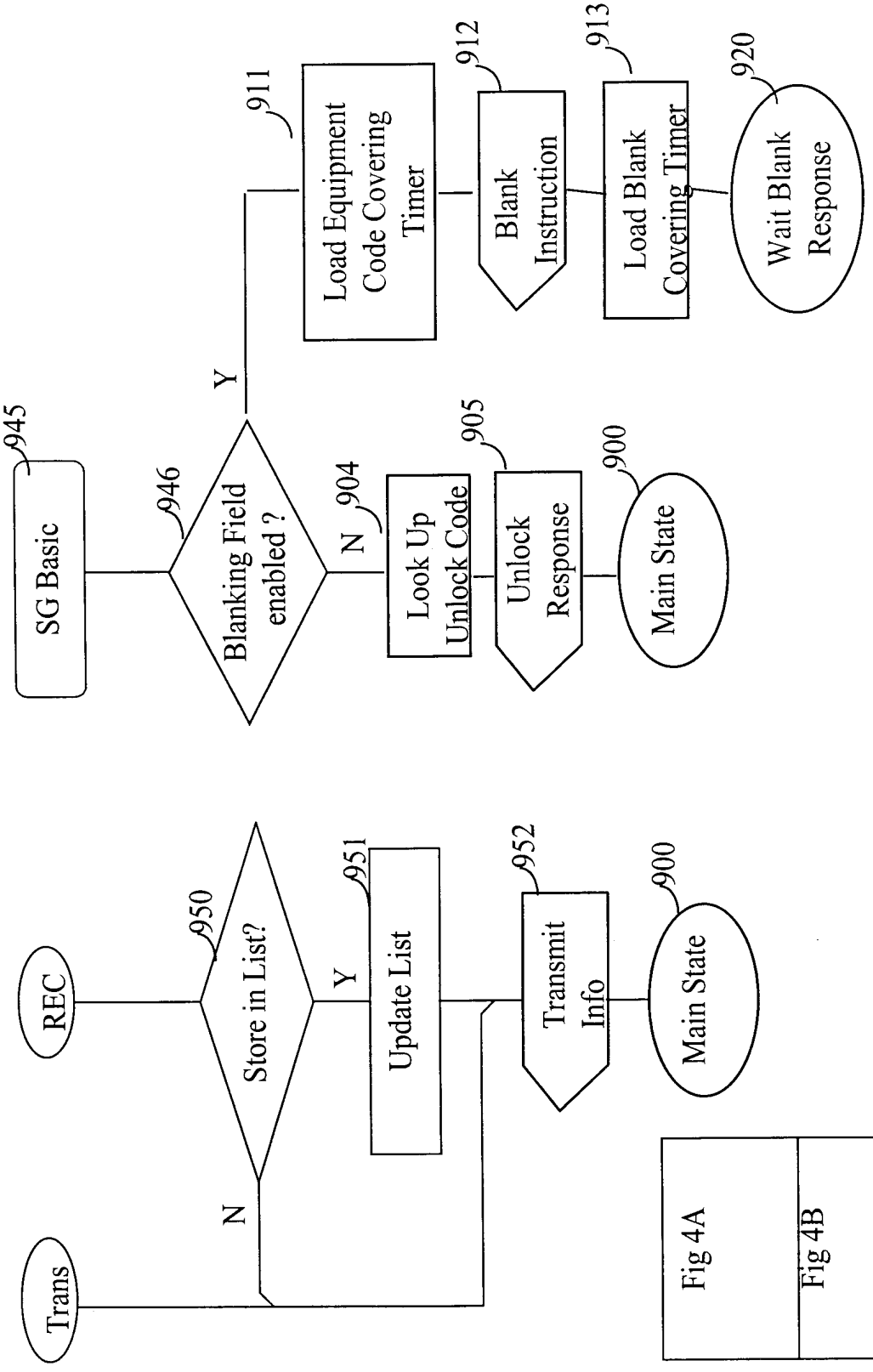

945
SG Basic
946
Blanking Field enabled ?
Y
911
Load Equipment Code Covering Timer
912
Blank Instruction
913
Load Blank Covering Timer
920
Wait Blank Response
N
904
Look Up Unlock Code
905
Unlock Response
900
Main State
REC
950
Store in List?
Y
951
Update List
952
Transmit Info
900
Main State
N
Trans
Fig 4A
Fig 4B

Fig4B

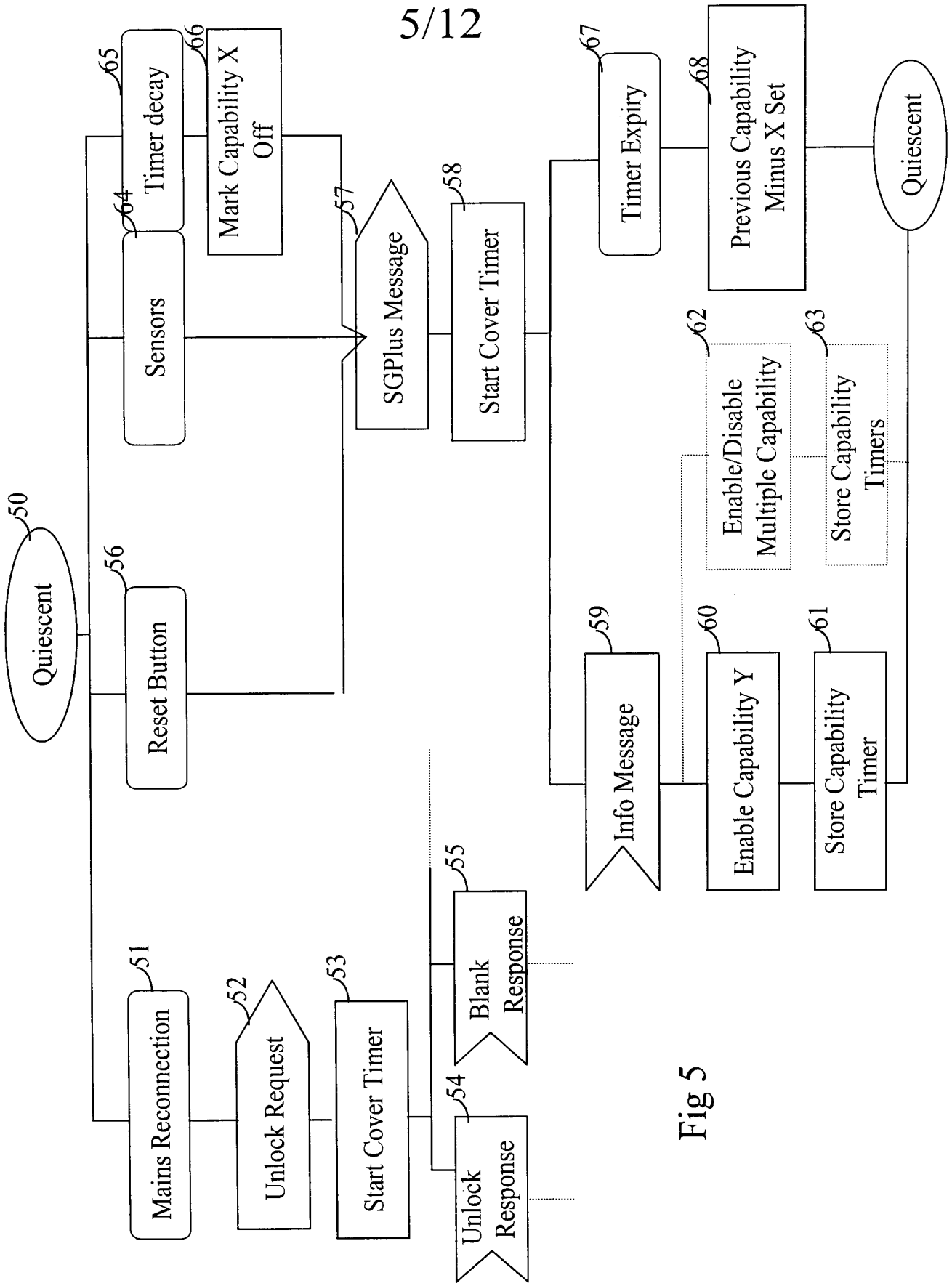

50
Quiescent
51
Mains Reconnection
52
Unlock Request
53
Start Cover Timer
54
Unlock Response
55
Blank Response
56
Reset Button
57
SGPlus Message
58
Start Cover Timer
59
Info Message
60
Enable Capability Y
61
Store Capability Timer
62
Enable/Disable Multiple Capability
63
Store Capability Timers
64
Sensors
65
Timer decay
66
Mark Capability X Off
67
Timer Expiry
68
Previous Capability Minus X Set
Quiescent

Fig 5

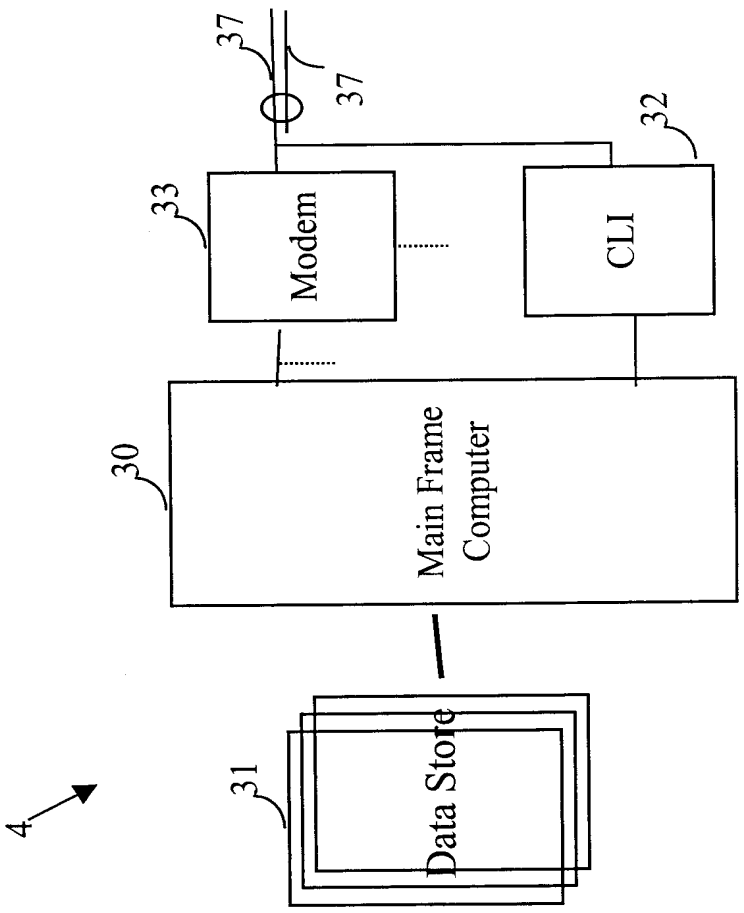
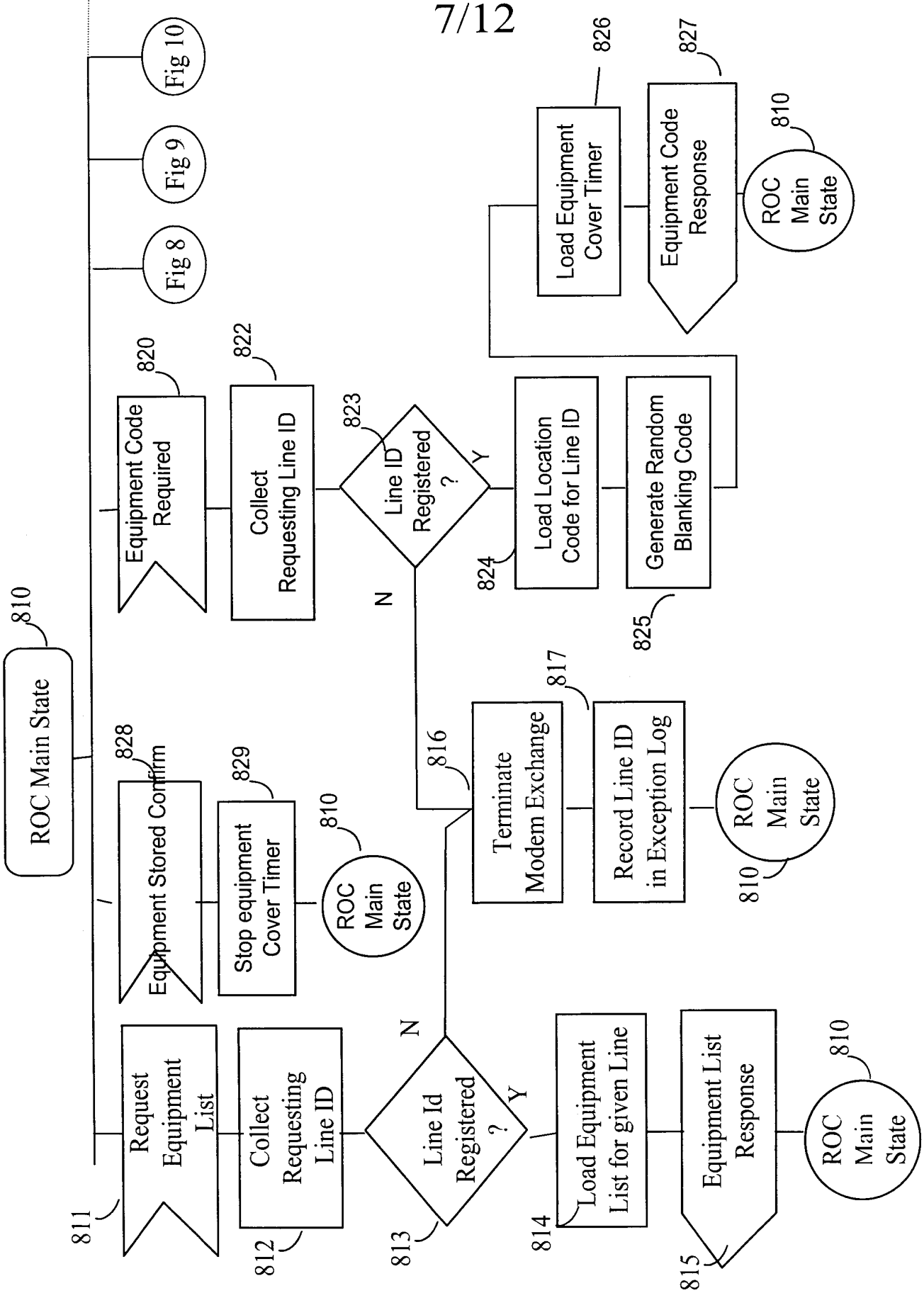


Fig 6


ROC Main State
810
Request Equipment List
811
Collect Requesting Line ID
812
Line Id Registered ?
813
N
Y
Load Equipment List for given Line
814
Equipment List Response
815
ROC Main State
810
Equipment Stored Confirm
828
Stop equipment Cover Timer
829
ROC Main State
810
Equipment Code Required
820
Collect Requesting Line ID
822
Line ID Registered ?
823
N
Y
Terminate Modem Exchange
816
Record Line ID in Exception Log
817
ROC Main State
810
Load Location Code for Line ID
824
Generate Random Blanking Code
825
Load Equipment Cover Timer
826
Equipment Code Response
827
ROC Main State
810
Fig 8
Fig 9
Fig 10

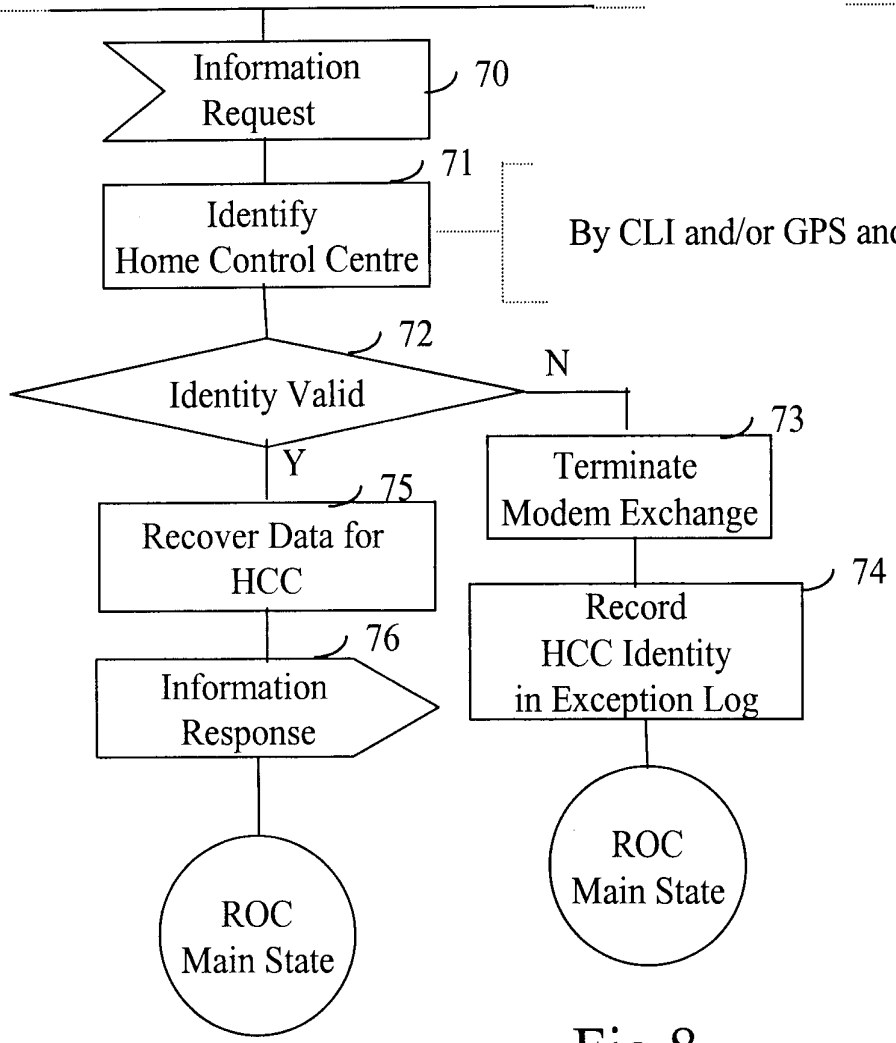

Information Request
70
Identify Home Control Centre
71
By CLI and/or GPS and/or Identity Data
72
Identity Valid
N
Y
73
Terminate Modem Exchange
74
Record HCC Identity in Exception Log
75
Recover Data for HCC
76
Information Response
ROC Main State
ROC Main State

Fig 8

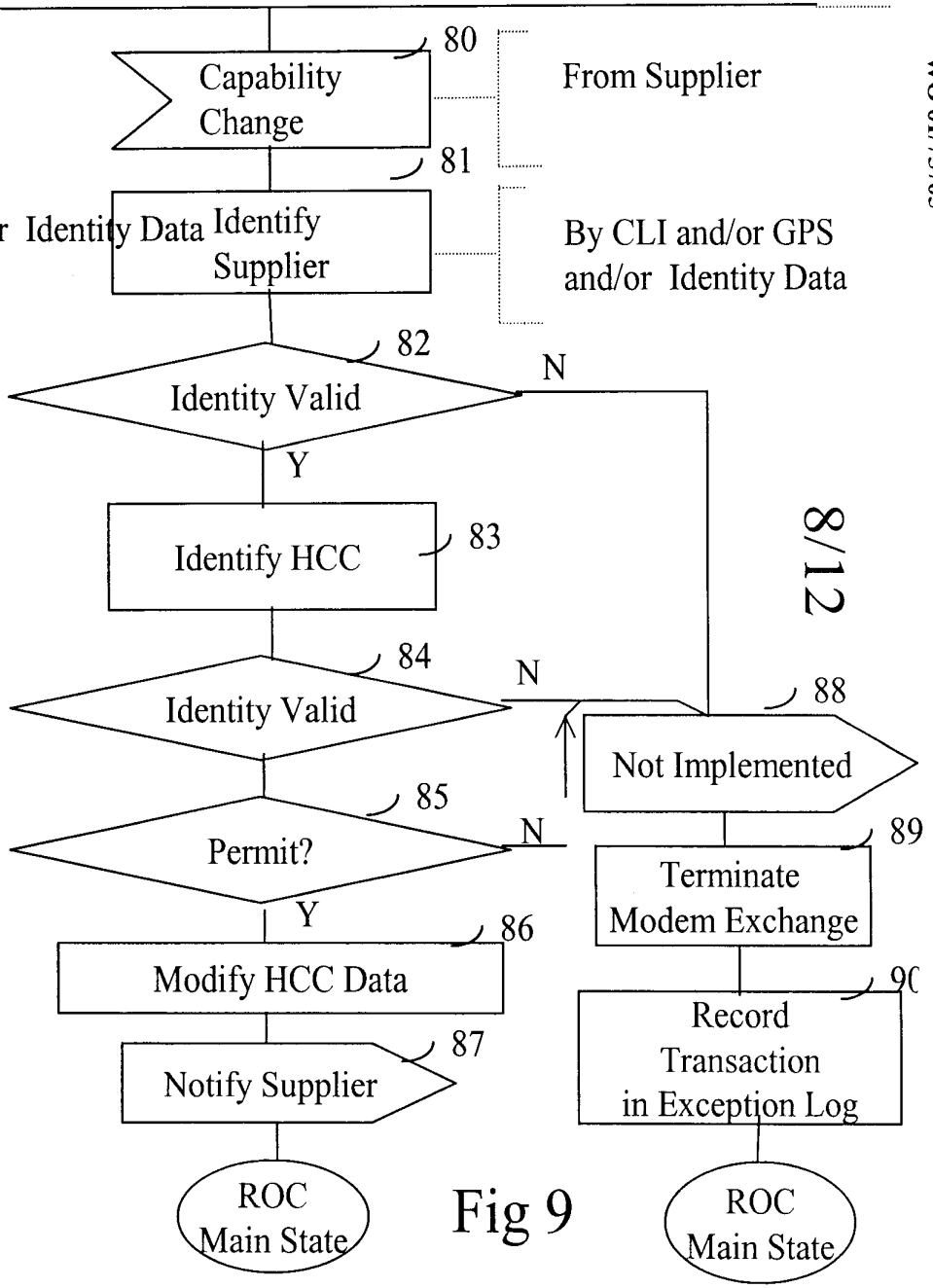
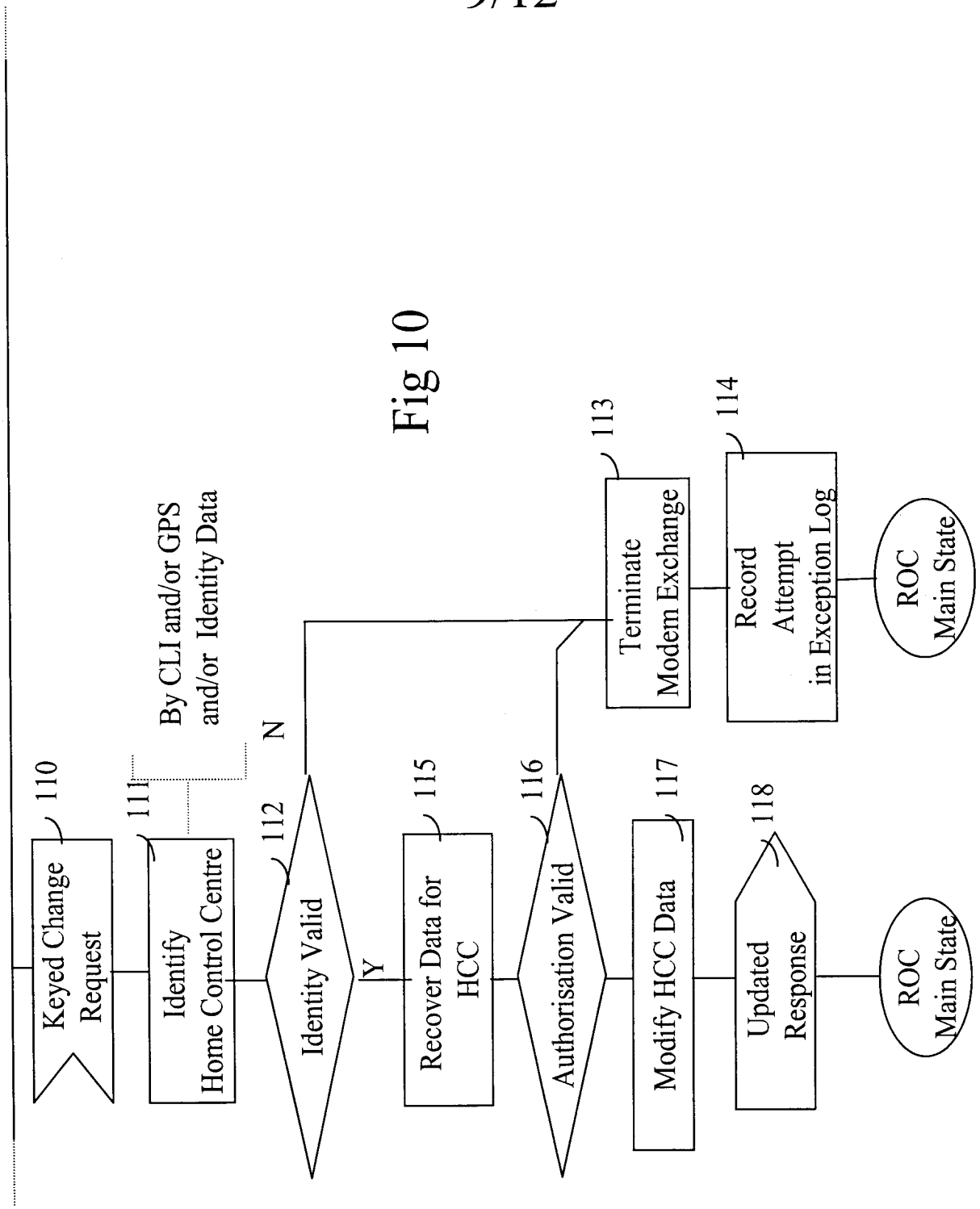

80
Capability Change
From Supplier
81
Identify Supplier
By CLI and/or GPS and/or Identity Data
82
Identity Valid
N
Y
83
Identify HCC
84
Identity Valid
N
88
Not Implemented
85
Permit?
N
89
Terminate Modem Exchange
Y
86
Modify HCC Data
90
Record Transaction in Exception Log
87
Notify Supplier
ROC Main State
ROC Main State

Fig 9

Fig 10


Keyed Change Request
110
Identify Home Control Centre
111
By CLI and/or GPS and/or Identity Data
Identity Valid
112
N
Y
Recover Data for HCC
115
Authorisation Valid
116
Terminate Modem Exchange
113
Record Attempt in Exception Log
114
ROC Main State
Modify HCC Data
117
Updated Response
118
ROC Main State

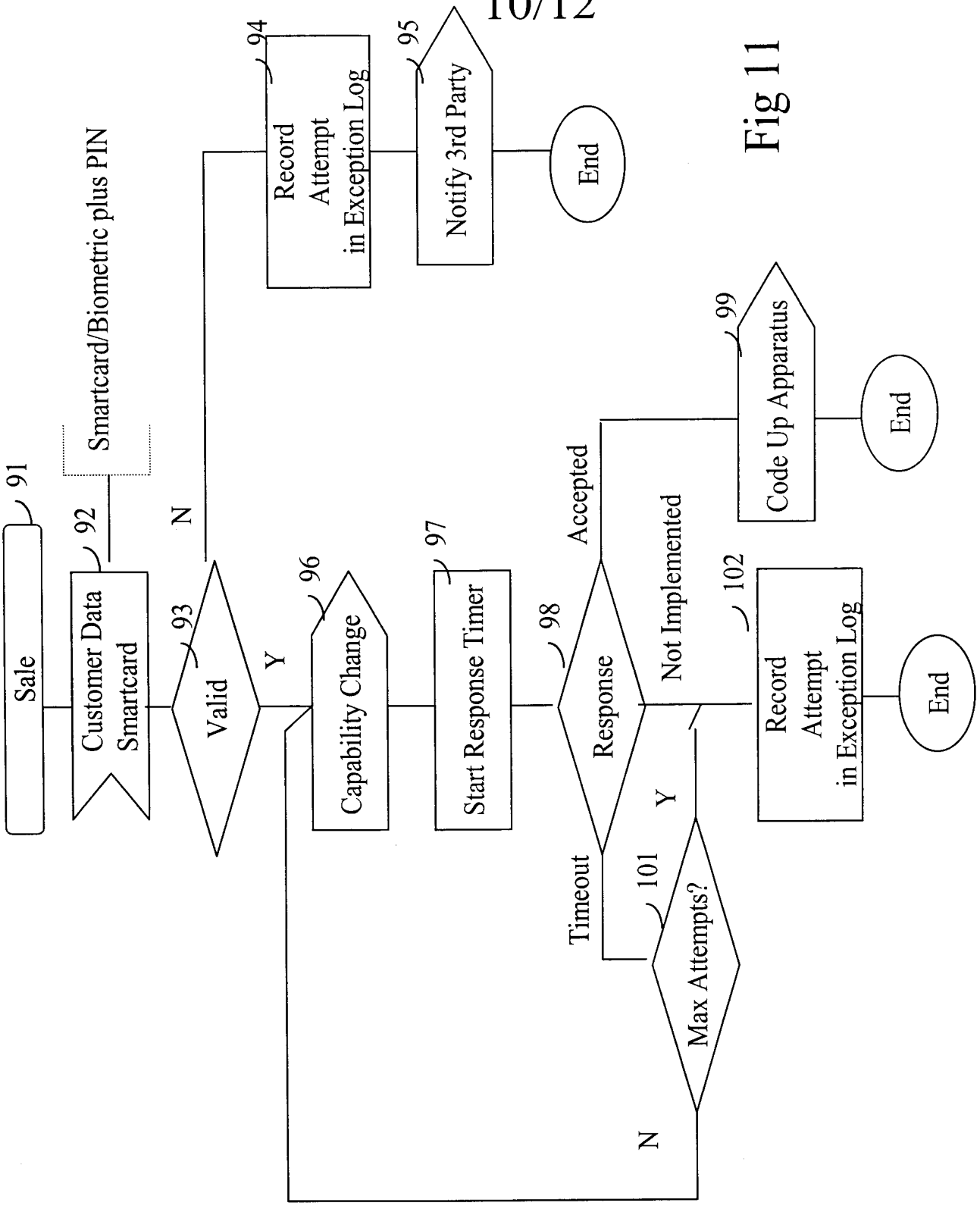

Sale
91
Customer Data Smartcard
92
Smartcard/Biometric plus PIN
Valid
93
N
Y
Record Attempt in Exception Log
94
Notify 3rd Party
95
End
Capability Change
96
Start Response Timer
97
Response
98
Accepted
Code Up Apparatus
99
End
Not Implemented
102
Record Attempt in Exception Log
End
Timeout
Max Attempts?
101
Y
N

Fig 11

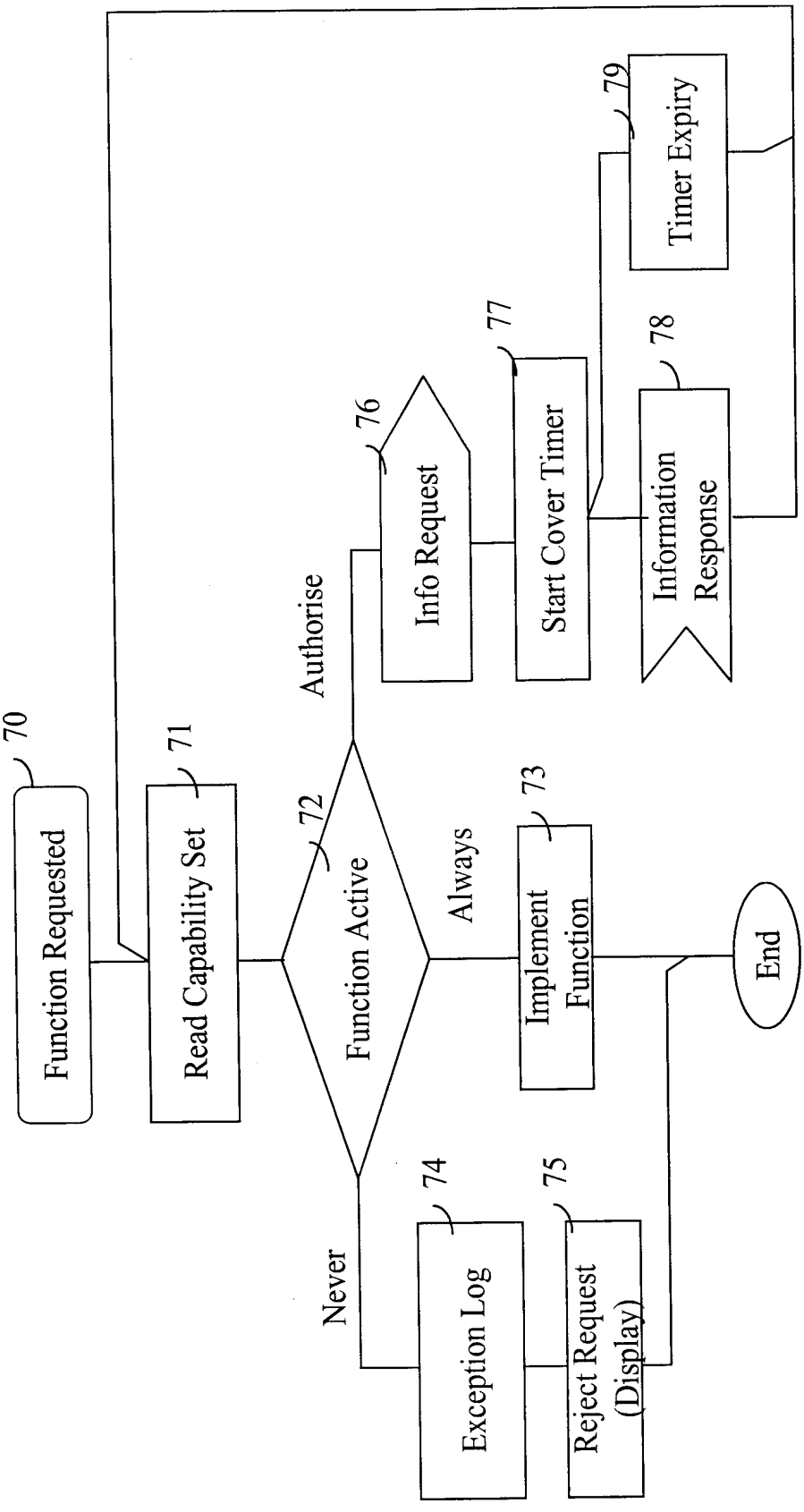

Function Requested
70
Read Capability Set
71
Function Active
72
Authorise
Always
Never
Implement Function
73
End
Exception Log
74
Reject Request (Display)
75
Info Request
76
Start Cover Timer
77
Information Response
78
Timer Expiry
79

Fig 12

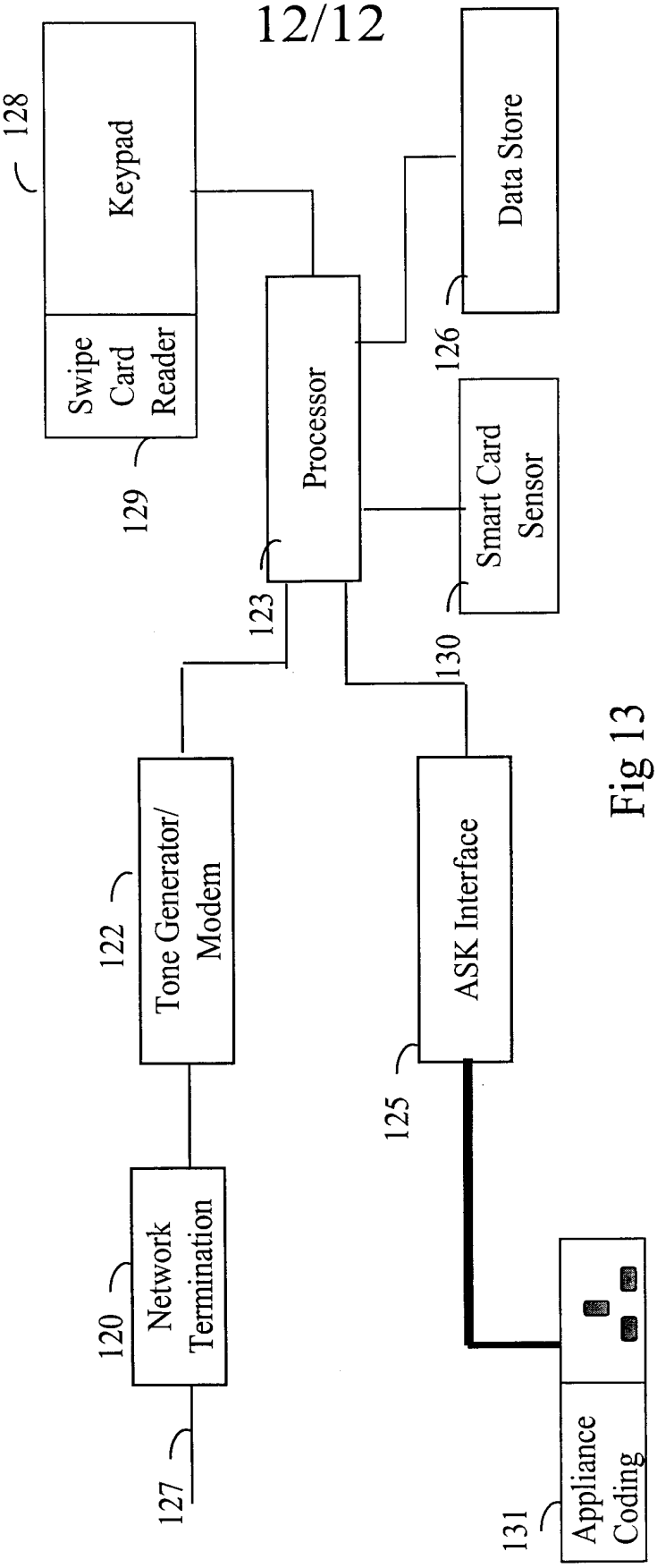

128
Keypad
Swipe Card Reader
129
Processor
123
Data Store
126
Smart Card Sensor
130
Tone Generator/ Modem
122
ASK Interface
125
Network Termination
120
127
Appliance Coding
131

Fig 13

INTERNATIONAL SEARCH REPORT

Inte. onal Application No
PCT/GB 01/00959

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G06F17/60 G08B13/14

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G06F G08B

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 00 16229 A (PREVIEW SYSTEMS INC) 23 March 2000 (2000-03-23) abstract page 1, line 9 -page 3, line 20 claims 1,4,6-9,11-18 figures 1,3-5	1-9
X	EP 0 869 462 A (BRITISH TELECOMM) 7 October 1998 (1998-10-07) cited in the application the whole document	1-9
X	EP 0 675 626 A (BRITISH TELECOMM) 4 October 1995 (1995-10-04) cited in the application the whole document	1-9

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
10 April 2001	18/04/2001

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	van der Weiden, A

1

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Inter ional Application No
PCT/GB 01/00959

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
X	WO 96 03728 A (KANG BALJIT SINGH) 8 February 1996 (1996-02-08) abstract page 1 -page 5 claims 1-7	1-9
X	WO 98 04967 A (BOWYER MARK DAVID JAMES ;COLLINS PETER DAVID (GB); ROYER KARL WILL) 5 February 1998 (1998-02-05) abstract page 3, line 6 -page 4, line 15 figures 2-4	1-9
X	EP 0 786 884 A (BOSCH GMBH ROBERT) 30 July 1997 (1997-07-30) abstract column 1, line 19 -column 2, line 34 claim 1 figure 1	1-9
A	EP 0 986 017 A (NCR INT INC) 15 March 2000 (2000-03-15) abstract column 1, line 3 -column 2, line 1 claim 1 figures 2,6	8,9

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

Inte. onal Application No
PCT/GB 01/00959

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 0016229 A	23-03-2000	AU 6239499 A	03-04-2000
EP 0869462 A	07-10-1998	AU 5995598 A	08-09-1998
		CN 1248338 T	22-03-2000
		EP 0960407 A	01-12-1999
		WO 9836391 A	20-08-1998
		US 6122350 A	19-09-2000
EP 0675626 A	04-10-1995	US 5729596 A	17-03-1998
WO 9603728 A	08-02-1996	AU 2986495 A	22-02-1996
		GB 2304443 A,B	19-03-1997
WO 9804967 A	05-02-1998	AU 1551097 A	20-02-1998
		EP 0912919 A	06-05-1999
EP 0786884 A	30-07-1997	DE 19602596 A	31-07-1997
EP 0986017 A	15-03-2000	JP 2000099828 A	07-04-2000